INFORMATION TECHNOLOGY LABORATORY
NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce
NO. 94 May 2006

CITA FURLANI SELECTED AS ITL DIRECTOR

NIST Director William Jeffrey has selected Cita Furlani as the new Director of the Information Technology Laboratory, effective April 30, 2006. Prior to her appointment, Furlani served as the NIST Chief Information Officer, Acting Director of the NIST Advanced Technology Program (ATP), and Director of the ATP Information Technology and Electronics Office. She began her career at NIST as a computer scientist and group leader in the Manufacturing Engineering Laboratory. Furlani also held the position of Director of the National Coordination Office for Networking and Information Technology R&D in the Executive Office of the President. See http://www.itl.nist.gov.

NIST Quantum Communications Team Marks Record-Breaking Milestone

The NIST Quantum Communications team, a partnership between ITL and the Physics Laboratory, has successfully implemented a complete fiber-based polarization encoded Quantum Key Distribution (QKD) system using the BB84 protocol. The initial trials of this system have resulted in a sifted key rate of over 4 Mbits/s at a 3.4% error rate with a quantum transmission rate of 625 Mbits/s through 1 km of fiber. Successful system operation has been demonstrated at up to 4 km of fiber with a reduction in sifted key rate and a slight increase in error rate. The NIST system generates keys at the highest speed ever reported so far, more than double the previous QKD speed record, also held by NIST. See http://www.nist.gov/public_affairs/releases/quantumfiber.htm.

ITL's New SAMATE Reference Dataset (SRD) Will Help Improve Trust and Confidence in Software

ITL recently launched the SAMATE Reference Dataset (SRD), which is a repository of thousands of samples of C, C++, and Java containing software security flaws. In some cases, the corrected (patched) versions are also available. The samples will be used to test software evaluation tools and help measure the effectiveness of such tools. Users can browse or search the samples and download samples they select. Approved users can submit test cases. The website is http://samate.nist.gov/SRD/.

Although the SRD currently contains source code only, the project goal is to cover all phases of software, from initial concept, through design and implementation, to acceptance, deployment, and operation. The dataset will eventually contain models, designs, and entire software applications. If you have suggestions for features, presentation, or usability, contact Michael Koo at (301) 975-2728, koo@nist.gov.

ITL Contributes to Humanoid Animation Standard

Sandy Ressler of ITL's Information Access Division was a key contributor to a Humanoid Animation (H-ANIM) standard, which was recently approved by the International Organization for Standardization (ISO). Developed with the Web3D Consortium, the standard, ISO/IEC 19774 Humanoid Animation (H-Anim), allows for the interoperable representation of human figures for animation and human modeling systems. Ressler integrated work from the CAESAR (human anthropometric survey) project with the 3D community to create a standard that will be used by both engineering design and entertainment industries.

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) ACTIVITIES

Secretary of Commerce Approves FIPS for Information Security

On March 9, 2006, Secretary of Commerce Carlos Gutierrez approved one revised and one new FIPS that are critical to improving the security of federal agencies and their information systems. FIPS 201-1, *Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors*, revises two sections of the original standard, Section 2.2, PIV Identify Proofing and Registration Requirements, and Section 5.3.1, PIV Card Issuance. These revisions clarify the identity proofing and registration process that federal agencies should follow when issuing identity credentials.

Also signed by the Secretary of Commerce on March 9th was FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 200 is one of a series of security standards and guidelines that ITL is developing to help federal agencies implement their responsibilities under the Federal Information Security Management Act (FISMA). To be used with other publications already issued by ITL (FIPS 199 and NIST Special Publication 800-53), FIPS 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements. Both FIPS are available at http://csrc.nist.gov/publications/fips/index.html.

INFORMATION TECHNOLOGY LABORATORY

If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:
ITL Newsletter
National Institute of Standards and Technology
100 Bureau Drive
Stop 8900
Gaithersburg, MD 20899-8900
You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

ITL Editor:
Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive
Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
E-mail: elizabeth.lennon@nist.gov

Request for Comments on Draft FIPS 186-3, *Digital Signature Standard (DSS)*

A Federal Register notice on March 13, 2006, announced for public review and comment a proposed draft FIPS 186-3, *Digital Signature Standard (DSS)*, available at http://csrc.nist.gov/publications/drafts.html. The proposed standard would revise and supersede FIPS 186-2, which specifies three algorithms to generate and verify digital signatures. With advances in technology, it is prudent to consider larger key sizes. Draft FIPS 186-3 allows the use of 1024, 2048, and 3072-bit keys. Other requirements have been added concerning the use of ANS X9.31 and ANS X9.62. In addition, the use of the RSA algorithm as specified in Public Key Cryptography Standard (PKCS) #1 (RSA Cryptography Standard) is allowed. Comments, due by June 12, 2006, may be sent to elaine.barker@nist.gov. The complete Federal Register notice is at http://www.itl.nist.gov/fipspubs/message.htm.

UPDATE ON NEW PUBLICATIONS

Our list of selected new publications, available online, features work in software security assurance, optical media longevity, personal identity verification, key establishment schemes, and system security planning.

Proceedings of Workshop on Software Security Assurance Tools, Techniques, and Metrics
By Paul Black, Michael Kass, and Elizabeth Fong
NIST Special Publication 500-265
February 2006
http://hissa.nist.gov/%7Eblack/Papers/NIST%20SP%20500-265.pdf

Proceedings of Defining the State of the Art in Software Security Tools Workshop
By Paul Black and Elizabeth Fong
NIST Special Publication 500-264
September 2005
http://hissa.nist.gov/%7Eblack/Papers/NIST%20SP%20500-264.pdf

These two publications present proceedings of two workshops that are part of a series in the NIST Software Assurance Measurement and Tool Evaluation (SAMATE) project. This project is partially funded by the Department of Homeland Security (DHS) to help identify and enhance software security assurance (SSA) tools. The workshops helped define the state of the art of SSA tools that detect security flaws and vulnerabilities and developed a standard reference dataset of programs with known flaws.

NIST/Library of Congress (LoC) Optical Media Longevity Study
By Oliver Slattery and Jian Zheng
NIST Special Publication 500-263
November 2005
http://www.itl.nist.gov/div895/loc/Public%20SP%20500-263%20November%202005.pdf

ITL and the Preservation Directorate at the Library of Congress (LoC) conducted a detailed investigation of the longevity of recordable Compact Disc (CD) and Digital Versatile Disc (DVD) media. This report outlines the procedural details of that investigation for estimating the life expectancy of information stored in CD-ROM, DVD-ROM, CD-R, DVD-R and DVD+R, as well as DVD-RW and DVD+RW discs. The test procedure uses accelerated aging techniques and statistical analysis to estimate the life expectancy (LE) of current recordable DVD and CD media.

Biometric Data Specification for Personal Identity Verification
By Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli
NIST Special Publication 800-76
February 2006
http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf

This document specifies technical acquisition and formatting requirements for the biometric credentials of FIPS 201-conformant Personal Identity Verification (PIV) systems, including the PIV Card itself. SP 800-76 enumerates required procedures and formats for fingerprints, fingerprint templates, and facial images by appropriate instantiation of values and practices generically laid out in published biometric standards.

Interfaces for Personal Identity Verification
By James Dray and Scott Guthery
NIST Special Publication 800-73-1
March 2006
http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1-March2006.pdf

FIPS 201, *Personal Identity Verification for Federal Employees and Contractors*, specifies that the identity credentials must be stored on a smart card. SP 800-73 contains technical specifications for smart card interfaces used to retrieve and use identity credentials. These specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying PIV data model, communication interface, and application programming interface (API). This revision contains minor changes to the original document.

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
By Elaine Barker, Don Johnson, and Miles Smid
NIST Special Publication 800-56A
March 2006
http://csrc.nist.gov/publications/nistpubs/800-56A/sp800-56A_March2006.pdf

This recommendation provides the specifications of key establishment schemes that are appropriate for use by the federal government, based on standards developed by the Accredited Standards Committee (ASC) X9, Inc.: American National Standard (ANS) X9.42 *Agreement of Symmetric Keys using Discrete Logarithm Cryptography* and ANS X9.63 *Key Agreement and Key Transport using Elliptic Curve Cryptography*. A key establishment scheme can be characterized as either a key agreement scheme or a key transport scheme. The asymmetric-key-based key agreement schemes in this recommendation are based on the Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) algorithms. In addition, an asymmetric-key-based key transport scheme is specified.

Guide for Developing Security Plans for Federal Information Systems
By Marianne Swanson, Joan Hash, and Pauline Bowen
NIST Special Publication 800-26, Revision 1
February 2006
http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

The objective of system security planning is to improve protection of information system resources. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and" Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA). NIST SP 800-18, Revision 1, gives updated guidance on security planning.

"ITL" Available Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send and e-mail message from your business e-mail account to listproc@nist.gov with the message subscribe itl-newsletter, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the newsletter sent to an e-mail address other than the FROM address, contact the ITL editor.

UPCOMING TECHNICAL CONFERENCES

Second Cryptographic Hash Workshop
As a follow-on to the first Cryptographic Hash Workshop held Oct. 31-Nov. 1, 2005, ITL plans to host a series of public workshops to focus on hash function research in preparation for developing additional hash function(s) through a public competition. The next workshop will be held as follows:

Dates: August 24-25, 2006 *(in conjunction with Crypto 2006)*
Place: University of California, Santa Barbara, California
Technical contact: Shu-jen Chang, (301) 975-2940, shu-jen.chang@nist.gov
Conference website: http://www.nist.gov/hash-function

Biometric Consortium Conference 2006 (BC2006)
BC2006 will address the important role that biometrics can play in the identification and verification of individuals in this age of heightened security and privacy by examining biometric-based solutions for homeland security (airport security, travel documents, visas, border control, prevention of ID theft) as well as the utilization of biometrics in other applications such as point of sale and large-scale enterprise network environments. BC2006 will provide a